PUBLICATION

NAIC Insurance Data Security Model Law to Be Presented for Adoption

Authors: Layna S. Cook Rush
September 07, 2017

Insurers and organizations regulated by state insurance departments need to be prepared to meet the requirements of the model data security law, which may be finalized this year. In late 2014, the National Association of Insurance Commissioners (NAIC) Executive Committee appointed a Cybersecurity Working Group to identify the focus for insurance regulatory activities related to cybersecurity. Last month, the NAIC Cybersecurity Working Group adopted the sixth draft of the Insurance Data Security Model Law (model law) as a final draft; it is anticipated that the model law will be presented to the NAIC Executive Committee for adoption at its Fall 2017 National Meeting, which is held in December.

The purpose of the model law is to establish standards for data security and the investigation of, and notification to, the state insurance commissioner of a "Cybersecurity Event" applicable to "Licensees." Licensee is broadly defined and includes all persons licensed, authorized to operate, or registered, or required to be licensed, authorized or registered pursuant to the insurance laws of the state. The definition encompasses insurers and producers. Additionally, other entities such as third-party administrators, utilization review companies and independent review organizations may be subject to the law if state insurance laws require their licensure or registration.

The model law requires licensees to conduct a risk assessment and adopt a comprehensive written information security program (unless the licensee has less than ten employees). As part of its information security program, each licensee must establish a written incident response plan designed to promptly respond to, and recover from, any Cybersecurity Event that compromises the confidentiality, integrity or availability of nonpublic information in its possession, the licensee's information systems or the continuing functionality of any aspect of the licensee's business or operations.

If a licensee has a board of directors, the board or appropriate board committee must oversee the development, implementation and maintenance of the information security program and ultimately approve the program. Additionally, an annual report on the overall status of the program and recommendations for changes must be provided to the board. Insurers are also required to annually submit a written statement to the insurance commissioner in their domiciliary state, certifying the insurer has an information security program that is in compliance with the model law. If a licensee has established and maintains an information security program that is in compliance with HIPAA, then it is considered to meet the model law's requirements for an information security program and only has to submit a written statement certifying its compliance with HIPAA.

The model law defines "Cybersecurity Event" as an event resulting in unauthorized access to, disruption or misuse of, an information system or information stored on such information system. It does not include the unauthorized acquisition of encrypted nonpublic information if the encryption, process or key was not also accessed or revealed. Also excluded from the definition is an event where the licensee has determined that the nonpublic information accessed by an unauthorized person has not been used or released and has been returned or destroyed. If a licensee learns that a Cybersecurity Event has or may have occurred, the licensee or an outside vendor and/or service provider designated to act on behalf of the licensee, is required to conduct an investigation. In certain circumstances, the licensee is required to notify the insurance commissioner within 72 hours of determining that a Cybersecurity Event has occurred. A licensee has the same notification

requirements when it learns that its third-party service provider has experienced a Cybersecurity Event. The model law defers to the state's data breach notification law to determine whether consumer notification is required.

Licensees who are required to comply with HIPAA should not find compliance with the model law onerous, as they should already have policies and procedures addressing the security of information systems. The model law will most likely require licensees subject to HIPAA to reexamine their current breach notification policies. Those entities who have not had a HIPAA compliant information security program should examine their current policies and practices addressing the security of their information systems in preparation for compliance with the law.